CLAIMS

1. A computing device having instantiated thereon a protected media path for delivering content from at least one source to at least one sink, the protected media path comprising:

a media base providing a protected environment in the computing device and including a common infrastructure of core components effectuating processing of content from any particular source and delivering the processed content to any particular sink, and also including a policy engine enforcing policy on behalf of each source, the policy corresponding to the content from the source and including rules and requirements for accessing and rendering the content, whereby the media base allows content to flow through the computing device in a protected fashion, and allows for arbitrary processing of the protected content in the computing device;

a source trust authority (SOTA) associated with and corresponding to each source of content, each SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path, decrypting the content from the source if necessary, and translating policy associated with the content from a native format into a format amenable to the policy engine if necessary; and

a sink trust authority (SITA) associated with and corresponding to each sink of content, each SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path, encrypting content to be delivered to the sink if necessary, and translating the policy associated with the content from the format of the policy engine into a format amenable to the sink if necessary, whereby the sink receives the content and corresponding policy, decrypts the received content if necessary, and renders same based on the received policy.

2. The computing device of claim 1 wherein the media base of the instantiated protected media path further includes at least one supplemental component providing additional protected functionality to the computing device.

3. The computing device of claim 1 further having instantiated thereon a media application selecting the content to be delivered, selecting each source for providing the content by way of the protected media path, if necessary selecting each sink to receive the provided content by way of the protected media path, actuating the media base to arrange the protected media path according to each selected source and each selected sink.

4. The computing device of claim 3 wherein the media application provides delivery commands to the media base to control delivery of the content from each selected source to each selected sink.

5. The computing device of claim 3 wherein the media base prevents the media application from having access to the content delivered within the protected media path.

6. The computing device of claim 3 wherein the media base prevents the media application from taking any action with respect to the content contrary to the policy corresponding to the content.

7. The computing device of claim 1 wherein each SOTA of the instantiated protected media path allows content thereof to be delivered through the protected media path 39 only if the SOTA is satisfied that the media base, the policy engine thereof, each employed component thereof, and each SITA of the protected media path is trustworthy and has rights to be in contact with the content based on the policy corresponding thereto.

8. The computing device of claim 7 wherein any element can be shown to be trustworthy based on a proffer of an acceptable token that vouches for the element.

9. The computing device of claim 8 wherein any element can be shown to be trustworthy based on a proffer of a verifiable digital certificate from an acceptable vouching authority.

10. The computing device of claim 8 wherein a trustworthy element is trusted to decide whether same can be in contact with the content based on the policy corresponding thereto and based on whether same can honor the policy corresponding to the content.

11. The computing device of claim 8 wherein a trustworthy element is trusted to respond truthfully to a rights-based query from another element.

12. A method of delivering content from a source to a sink by way of a computing device, the method comprising:

an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink;

the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path including:

the media base;

a source trust authority (SOTA) associated with and corresponding to the source, the SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path, decrypting the content from the source if necessary, and translating policy

associated with the content from a native format into a format amenable to the policy engine if necessary; and

a sink trust authority (SITA) associated with and corresponding to the sink, the SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path, encrypting content to be delivered to the sink if necessary, and translating the policy associated with the content from the format of the policy engine into a format amenable to the sink if necessary, whereby the sink receives the content and corresponding policy, decrypts the received content if necessary, and renders same based on the received policy;

the SOTA on behalf of the source establishing trust with respect to the protected media path;

the SOTA upon trust being established with respect to the protected media path propagating policy corresponding to the content to be delivered to the protected media path;

the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path;

the SOTA deciding whether the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same;

the media base informing the application whether the particular type of action can be taken, and if so the application proceeding by commanding the media base to perform such type of action.

13. The method of claim 12 wherein the media base establishing the protected media path comprises the media base selecting core components thereof that are to handle and operate on the content while being delivered through the protected media path, the core components providing core functionality to the media base.

14. The method of claim 13 wherein the media base establishing the protected media path further comprises the media base selecting supplemental components thereof that are to handle and operate on the content while being delivered through the protected media path, the supplemental components providing supplemental functionality to the media base.

15. The method of claim 12 wherein the SOTA establishing trust with respect to the protected media path comprises:

the SOTA establishing trust with a policy engine of the media base;

the trusted policy engine establishing trust with every other element of the protected media path including the SITA.

16. The method of claim 15 wherein establishing trust with any element comprises receiving a proffer of an acceptable token that vouches for the element.

17. The method of claim 16 wherein establishing trust with any element comprises receiving a proffer of a verifiable digital certificate from an acceptable vouching authority.

18. The method of claim 12 wherein the SOTA propagating policy corresponding to the content to be delivered to the protected media path comprises:

the SOTA propagating policy to a policy engine of the media base;

the policy engine as necessary determining that each element of the protected media path including the SITA satisfies the policy.

19. The method of claim 18 wherein if the policy engine determines that a particular element of the protected media path does not satisfies

the policy, the policy engine performs an action selected from a group consisting of refusing such element access to the content and preventing content from being delivered through the protected media path.

20. The method of claim 12 wherein the SOTA propagating policy corresponding to the content to be delivered to the protected media path comprises:

the SOTA propagating policy to a policy engine of the media base;

the policy engine propagating the policy to the SITA in the protected media path; and

the SITA as a trusted element of the protected media path abiding by such policy.

21. The method of claim 12 comprising the SOTA determining from the SITA the particular type of action to be taken with the content as delivered through the protected media path.

22. The method of claim 12 comprising the SOTA deciding whether the particular type of action can be taken with the content based on the policy corresponding thereto.

23. The method of claim 12 further comprising:

the SOTA obtaining the content from the source in an encrypted form, decrypting the encrypted content, and delivering the decrypted content to the media base;

the media base processing the decrypted content as necessary and delivering the processed content to the SIAT; and

the SITA encrypting the processed content and delivering the encrypted processed content to the sink.